1773

Novae demonstrationes circa resolutionem numerorum in quadrata

Leonhard Euler

NOVAE DEMONSTRATIONES CIRCA RESOLUTIONEM NUMERORUM IN QUADRATA[1])

Commentatio 445 indicis ENESTROEMIANI
Nova acta eruditorum 1773, p. 193—211
Acta academiae scientiarum Petropolitanae 1777: II, 1780, p. 48—69

1. Quum saepe et multum in hoc argumento fuissem occupatus neque tamen ea demonstratio, quam olim[2]) dederam circa resolutionem omnium numerorum in quatuor vel pauciora quadrata, mihi ipsi penitus satisfecisset, eo maiore ardore evolvi demonstrationem, quam Celeb. D. LAGRANGE[3]) nuper in primo volumine Novorum Actorum Acad. sc. Boruss. huius theorematis tradidit, quam utique negotium perfecisse sum admiratus, etiamsi eius momenta nimis longe repetita et vehementer operosa viderentur.

---

1) Haec dissertatio primum Novis actis eruditorum, deinde vero Actis academiae scientiarum Petropolitanae inserta est. Editioni nostrae subest editio posterior, quae a priore nonnullis locis paulo discrepat (vide *Redaktionsplan für die Eulerausgabe*, Jahresber. d. Deutschen Mathem.-Verein. **19**, 1910, Zweite Abt., p. 94). F. R.

2) Vide Commentationem 242 (indicis ENESTROEMIANI): *Demonstratio theorematis FERMATIANI omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*, Novi comment. acad. sc. Petrop. **5** (1754/5), 1760, p. 13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 338. F. R.

3) I. L. LAGRANGE, *Démonstration d'un théorème d'arithmétique*, Nouv. mém. de l'acad. d. sc. de Berlin (1770), 1772, p. 123; *Oeuvres de LAGRANGE*, publiées par les soins de M. I.-A. SERRET t. III, p. 189. F. R.

2. Lectoribus autem haud ingratum fore arbitror, si praecipua momenta, quibus haec demonstratio innititur, hic breviter et concinne proposuero. Postquam Celeb. Auctor hoc lemma praemisit, quodsi duae summae binorum quadratorum $pp+qq$ et $rr+ss$ communem habeant divisorem ϱ neque tamen singula quadrata per eum dividi queant, tum non solum ipsum hunc divisorem ϱ, sed etiam ambos quotos $\frac{pp+qq}{\varrho}$ et $\frac{rr+ss}{\varrho}$ fore summas duorum quadratorum, progreditur ad theorema demonstrandum, *quodsi summa quatuor quadratorum* $P^2+Q^2+R^2+S^2$ *divisibilis fuerit per numerum quemcumque* A *neque tamen singula quadrata per eum sint divisibilia, tum ipsum hunc numerum* A *fore summam quatuor quadratorum,* cuius demonstratio sequentibus continetur ratiociniis.

I. Posito quoto ex illa divisione oriundo $=a$, ut sit

$$Aa = P^2+Q^2+R^2+S^2,$$

si forte eveniat, ut binae formulae P^2+Q^2 et R^2+S^2 habeant communem divisorem ϱ, quem ergo etiam numerus a continebit, ponit $a=b\varrho$, ut fiat

$$Ab = \frac{P^2+Q^2}{\varrho} + \frac{R^2+S^2}{\varrho};$$

quae formulae quum per lemma praemissum sint summae duorum quadratorum, habebitur huiusmodi aequatio

$$Ab = pp+qq+rr+ss,$$

ubi formulae $pp+qq$ et $rr+ss$ non amplius habebunt factorem communem.

II. Tum vero ponit $pp+qq=t$ et $rr+ss=u$, ut sit $Ab=t+u$, quam aequationem ducit in t faciendo $Abt=tt+tu$; et quia tu etiam est summa duorum quadratorum, puta $xx+yy$, sumendo scilicet $x=pr+qs$ et $y=ps-qr$, fiet

$$Abt = tt+xx+yy.$$

III. Nunc per numeros t et b, quippe qui inter se sunt primi, ambos x et y ita exprimi posse observat, ut sit $x=\alpha t+\gamma b$ et $y=\beta t+\delta b$; ubi quum litterae α, β, γ, δ infinitis modis accipi queant sive negative sive positive, inter earum valores tales certe dabuntur, ut sit $\alpha<\frac{1}{2}b$ et $\beta<\frac{1}{2}b$.

IV. His iam valoribus pro x et y substitutis resultabit ista aequatio

$$Abt = tt(1 + \alpha\alpha + \beta\beta) + 2bt(\alpha\gamma + \beta\delta) + bb(\gamma\gamma + \delta\delta).$$

Quae expressio quum divisibilis esse debeat per b neque tamen in primo membro tt hanc divisionem admittat, necesse est, ut ibi formula $1 + \alpha\alpha + \beta\beta$ factorem habeat b; eodem modo etiam in ultimo membro factorem $\gamma\gamma + \delta\delta$ divisibilem per t esse necesse est. Ponatur ergo $1 + \alpha\alpha + \beta\beta = ba'$, et quia uterque numerus α et β minor est quam $\frac{1}{2}b$, manifestum est fore $a' < \frac{1}{2}b + \frac{1}{b}$; facta ergo divisione per b erit

$$At = a'tt + 2t(\alpha\gamma + \beta\delta) + b(\gamma\gamma + \delta\delta).$$

V. Multiplicetur nunc haec aequatio per a', ut prodeat

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + a'b(\gamma\gamma + \delta\delta),$$

et in ultimo membro loco $a'b$ scribendo $1 + \alpha\alpha + \beta\beta$ fiet

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + (\alpha\alpha + \beta\beta)(\gamma\gamma + \delta\delta) + \gamma\gamma + \delta\delta,$$

quae expressio in sequentia quatuor quadrata resolvetur

$$Aa't = (a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2 + \gamma^2 + \delta^2;$$

ubi quum summa binorum postremorum quadratorum $\gamma^2 + \delta^2$ divisibilis sit per numerum t, necesse est, ut summa duorum priorum quoque divisibilis sit per t, ita ut hic duae binorum quadratorum summae occurrant communem divisorem t habentes; quare si per t dividatur, ambo illi quoti itidem erunt summae binorum quadratorum.

VI. Quodsi ergo ponamus

$$\frac{(a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2}{t} = p'^2 + q'^2 \quad \text{et} \quad \frac{\gamma^2 + \delta^2}{t} = r'^2 + s'^2,$$

habebimus

$$Aa' = p'^2 + q'^2 + r'^2 + s'^2.$$

In hac autem formula Aa', si cum prima Aa comparetur, numerus a' multo minor erit quam a, quandoquidem $b < a$ et $a' < \frac{1}{2}b$. Simili modo ergo per-

venire licebit ad formulam Aa'', ubi a'' multo minor erit quam a', sicque tandem perveniri necesse est ad formulam $A \cdot 1$, ita ut iam ipse numerus A reperiatur aequalis summae quatuor quadratorum.

3. Demonstrato hoc theoremate insuper ostendi oportet proposito quocumque numero primo semper exhiberi posse summam quatuor quadratorum per eum divisibilem, quorum tamen singula quadrata divisionem non admittant. Atque hoc etiam Cel. LAGRANGE modo maxime ingenioso demonstrat, qui autem tantopere est abstrusus et prolixus, ut eius momenta breviter et dilucide nequaquam exhiberi possint. Nunc igitur famosum illud theorema sive BACHETI[1]) sive FERMATII, *quod omnis numerus in quadrata quatuor vel pauciora resolvi possit*, pro perfecte demonstrato est habendum. Quia enim pro numero primo quocumque semper dari potest summa quatuor quadratorum per illum divisibilis, omnes numeri primi summae erunt quatuor pauciorumve quadratorum, et quia iam dudum[2]) demonstratum est producta ex duobus pluribusve numeris, qui singuli sunt summae quatuor pauciorumve quadratorum, quoque in quatuor quadrata dispertiri posse, solidissime iam est evictum omnes plane numeros esse summas quatuor quadratorum pauciorumve.

4. Quamvis omnino nefas esset quicquam contra soliditatem et rigorem harum demonstrationum excipere, tamen nemo negabit eas nimis longe esse repetitas neque ipsa fundamenta et rationes singulorum ratiociniorum, quibus hae demonstrationes sint compositae, haud levi obscuritate esse involutas, ita ut etiamnunc merito clariores et perceptu faciliores demonstrationes desiderare liceat. Quo quidem desiderio summae laudi, quam istae demonstrationes merentur, nihil detrahi est censendum.

5. Quum igitur, postquam hoc argumentum de novo perpendissem, in novas et satis planas eorundem theorematum demonstrationes mihi incidere contigerit, iis, qui hoc studio delectantur, communicatio harum novarum demonstrationum certe gratissima fore videtur; quocirca eas hoc loco, quantum potero, breviter et dilucide sum propositurus. Ac primo quidem a theoremate illo notissimo simulque plenissime demonstrato, quo omnes divi-

1) Vide notam 4 p. 358 voluminis praecedentis. F. R.

2) Vide § 93 Commentationis 242 nota 2 p. 218 laudatae. F. R.

sores cuiusque summae duorum quadratorum inter se primorum ipsi summae duorum quadratorum aequales affirmantur, incipiam, cum quod haec nova[1]) demonstratio simplicitate se maxime commendat, tum vero quod iisdem vestigiis insistendo demonstratio facile ad quatuor quadrata extendi potest.

LEMMA 1

6. *Productum ex duabus summis binorum quadratorum itidem est summa duorum quadratorum.*

Nam si illud productum fuerit $(aa+bb)(\alpha\alpha+\beta\beta)$ et capiatur

$$A = a\alpha + b\beta \quad \text{et} \quad B = a\beta - b\alpha,$$

utique erit

$$(aa+bb)(\alpha\alpha+\beta\beta) = AA + BB.$$

THEOREMA 1

Si numerus N fuerit divisor summae duorum quadratorum P^2+Q^2 inter se primorum, tum ipse ille numerus N erit summa duorum quadratorum.

DEMONSTRATIO

Quo hanc demonstrationem facilius etiam in numeris exsequi liceat, cui forte libuerit, observo, quantumvis magni fuerint numeri P et Q, ex iis semper aliam summam duorum quadratorum $pp+qq$ formari posse, quorum radices p et q semissem numeri propositi N non superent. Nam si ponatur

$$P = fN \pm p \quad \text{et} \quad Q = gN \pm q,$$

notissimum est numeros p et q ita sumi posse, ut semissem $\frac{1}{2}N$ non superent. Quum igitur iam sit

$$PP + QQ = NN(ff+gg) + 2N(\pm fp \pm gq) + pp + qq$$

1) Confer illius theorematis demonstrationem priorem, quae continetur in Commentatione 228 (indicis Enestroemiani): *De numeris, qui sunt aggregata duorum quadratorum*, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295. F. R.

haecque expressio per N sit divisibilis, evidens est etiam hanc binorum quadratorum summam per N divisibilem fore. Hoc praemisso ipsam demonstrationem sequentibus momentis complectar.

I. Quum igitur ista formula $pp + qq$ divisorem habeat N, ponendo quotum $= n$ habebimus

$$Nn = pp + qq,$$

ubi ergo n minor erit quam $\frac{1}{2}N$, quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$.

II. Iam istos numeros p et q per numerum n ita exprimere licebit, ut sit

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n,$$

ubi admissis etiam numeris negativis pro a et b eos infra $\frac{1}{2}n$ deprimere licebit, uti iam initio observavimus. Tum vero erit

$$Nn = aa + bb + 2n(a\alpha + b\beta) + nn(\alpha\alpha + \beta\beta),$$

et quia in lemmate praemisso erat $a\alpha + b\beta = A$, fiet

$$Nn = aa + bb + 2nA + nn(\alpha\alpha + \beta\beta).$$

III. Huius ergo expressionis primum membrum $aa + bb$ factorem habeat necesse est n, quia reliqua membra iam per se divisorem n admittunt. Statuamus ergo

$$aa + bb = nn',$$

et quia $a < \frac{1}{2}n$ et $b < \frac{1}{2}n$ ideoque $nn' < \frac{1}{2}nn$, erit utique $n' < \frac{1}{2}n$. Hoc autem valore substituto et divisione per n facta prodit

$$N = n' + 2A + n(\alpha\alpha + \beta\beta).$$

IV. Hanc aequationem ducamus in n', et quia $nn' = aa + bb$, postremum membrum per lemma praemissum reducitur ad

$$nn'(\alpha\alpha + \beta\beta) = (aa + bb)(\alpha\alpha + \beta\beta) = AA + BB,$$

ita ut nunc habeamus

$$Nn' = n'n' + 2n'A + AA + BB,$$

quae expressio manifesto est summa duorum quadratorum, scilicet

$$Nn' = (n' + A)^2 + B^2.$$

V. Quum ergo initio fuisset productum Nn summa duorum quadratorum indeque hic elicuerimus productum minus Nn' etiam aequale summae duorum quadratorum, eodem modo ad talia producta continuo minora pertingere licebit, scilicet Nn'', Nn''' etc. Necesse igitur est, ut tandem ad productum minimum, scilicet $N \cdot 1$, perveniatur, sicque ipse numerus propositus N quoque erit summa duorum quadratorum.

COROLLARIUM

Mirum forsitan videbitur, quum perventum fuerit ad huiusmodi numerum $n' = 1$, quomodo sequentes operationes similes se sint habiturae; id quod facile patebit sumendo statim $n = 1$; tum enim habebitur $p = a + \alpha \cdot 1$ et $q = b + \beta \cdot 1$, ubi manifesto sumere licet $a = 0$ et $b = 0$, quippe quo pacto fiunt $< \frac{1}{2}$; tum vero ob $aa + bb = 0$ utique erit $n' = 0$ atque hic progressio ulterior nostri ratiocinii sponte sistitur.

SCHOLION

Eodem modo demonstrari potest omnes numeros vel huius formae $pp + 2qq$ vel $pp + 3qq$ alios non admittere divisores, nisi qui ipsi sint eiusdem formae, siquidem numeri p et q fuerint primi inter se.[1]) Neque vero hoc ratiocinium ad formas altiores, veluti $pp + 5qq$, $pp + 6qq$, extendi potest, quia tum non amplius sequeretur numerum n' necessario minorem esse quam n. Priorum igitur illorum casuum demonstrationes hic apponamus.

LEMMA 2

7. *Productum ex duobus numeris huius formae $pp + 2qq$ semper est numerus eiusdem formae.*

Si enim tale productum proponatur $(aa + 2bb)(\alpha\alpha + 2\beta\beta)$ et sumatur

$$A = a\alpha + 2b\beta \quad \text{et} \quad B = a\beta - b\alpha,$$

tum utique erit

$$AA + 2BB = (aa + 2bb)(\alpha\alpha + 2\beta\beta).$$

1) Vide ad has formas $pp + 2qq$ et $pp + 3qq$ Commentationes 256 et 272 (indicis Enestroemiani): *Specimen de usu observationum in mathesi pura*, Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185, et *Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 105; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 459 et 556. F. R.

THEOREMA 2

Si N fuerit divisor numeri $pp + 2qq$ et p et q sint primi inter se, tum etiam ipse numerus N in tali forma continebitur.

DEMONSTRATIO

Hic iterum numeros p et q infra semissem numeri N deprimere licebit et nostra demonstratio sequenti modo procedet.

I. Sit

$$Nn = pp + 2qq,$$

et quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, erit $n < \frac{3}{4}N$. Iam ponatur ut ante

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n,$$

ubi a et b capi poterunt minores quam $\frac{1}{2}n$, hincque habebitur

$$Nn = aa + 2bb + 2n(a\alpha + 2b\beta) + nn(\alpha\alpha + 2\beta\beta),$$

quae forma per lemma praemissum reducitur ad

$$Nn = aa + 2bb + 2nA + nn(\alpha\alpha + 2\beta\beta).$$

II. Hic igitur primum membrum $aa + 2bb$ factorem habebit n, unde posito

$$aa + 2bb = nn'$$

erit utique $n' < \frac{3}{4}n$. Hoc iam valore substituto et per n diviso fiet

$$N = n' + 2A + n(\alpha\alpha + 2\beta\beta).$$

III. Multiplicetur per n' atque per lemma praemissum habebitur

$$nn'(\alpha\alpha + 2\beta\beta) = (aa + 2bb)(\alpha\alpha + 2\beta\beta) = AA + 2BB,$$

ita ut nunc habeatur

$$Nn' = n'n' + 2n'A + AA + 2BB,$$

quae forma manifesto reducitur ad hanc

$$Nn' = (n' + A)^2 + 2BB,$$

ideoque itidem numerus formae $pp + 2qq$.

IV. Quum ergo sit $n' < n$, simili modo ad producta sequentia pervenire licebit Nn'', Nn''' etc., ita ut numeri n, n', n'', n''' etc. continuo decrescant. Tandem ergo perveniatur necesse est ad formam $N \cdot 1$, ita ut ipse numerus N quoque in eadem forma $pp + 2qq$ contineatur.

LEMMA 3

8. *Productum ex duobus numeris formae* $pp + 3qq$ *semper ad similem formam reduci potest.*

Sit enim tale productum $(aa + 3bb)(\alpha\alpha + 3\beta\beta)$ et capiatur

$$A = a\alpha + 3b\beta \quad \text{et} \quad B = a\beta - b\alpha;$$

manifesto habebitur

$$AA + 3BB = (aa + 3bb)(\alpha\alpha + 3\beta\beta).$$

THEOREMA 3

Si N *fuerit divisor numeri* $pp + 3qq$, *ubi* p *et* q *sint numeri primi inter se, tum ipse numerus* N *ad eandem formam reduci poterit.*

DEMONSTRATIO

Quum iterum spectare liceat $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, ipsa forma $pp + 3qq$ minor erit quam N^2. Posito ergo

$$pp + 3qq = Nn$$

factor n minor erit quam N, quae quidem reductio ad demonstrationem non est necessaria; ea enim aeque procedet, etiamsi fuerit $n > N$, uti sequitur.

I. Posito iam

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n$$

hic numeros a et b minores statuere licet quam $\frac{1}{2}n$, saltem non maiores; tum autem erit

$$Nn = aa + 3bb + 2n(a\alpha + 3b\beta) + nn(\alpha\alpha + 3\beta\beta),$$

quae per lemma praemissum fit

$$Nn = aa + 3bb + 2nA + nn(\alpha\alpha + 3\beta\beta).$$

II. Necesse igitur est, ut primum membrum $aa + 3bb$ factorem habeat n; quare posito

$$aa + 3bb = nn'$$

hic numerus n' certe minor erit quam n, saltem non maior; tum vero facta divisione per n prodibit

$$N = n' + 2A + n(\alpha\alpha + 3\beta\beta).$$

III. Multiplicemus iam per n' et postremum membrum

$$nn'(\alpha\alpha + 3\beta\beta) = (aa + 3bb)(\alpha\alpha + 3\beta\beta)$$

per lemma praemissum fit $AA + 3BB$ sicque habebimus

$$Nn' = n'n' + 2n'A + AA + 3BB,$$

quae expressio manifesto reducitur ad hanc

$$Nn' = (n' + A)^2 + 3BB.$$

IV. Quum igitur Nn' iterum sit formae $pp + 3qq$ et $n' < n$, eodem modo continuo progredi licebit ad continuo minora producta Nn'', Nn''' etc., donec tandem ad ultimum $N \cdot 1$ perveniatur; atque adeo demonstratum est fore ipsum numerum N formae $pp + 3qq$.

COROLLARIUM 1

Fundamentum huius demonstrationis ut et praecedentium in hoc consistit, quod a quolibet numero n perveniatur ad alium n' multo minorem, id quod

iis casibus, quibus n est numerus satis magnus, per se est perspicuum. Quin etiam haec ratio eo casu valet, quo $n = 1$; quia enim tum sumi poterit $a = 0$ et $b = 0$, ob $nn' = 0$ utique fiet $n' = 0$.

Interim tamen pro hoc theoremate singularis plane casus occurrit, quando in progressione numerorum n, n', n'' etc. tandem ad binarium pervenitur; qui casus eo maiorem attentionem meretur, quod nusquam alibi occurrat.[1])

COROLLARIUM 2

Pro hoc ergo casu statuamus statim $n = 2$ et manifestum est in formula $pp + 3qq$ utrumque numerum p et q esse debere imparem; utrumque enim parem assumere non licet, quia p et q inter se primi statuuntur. Quare quum hic fieri debeat $p = a + 2\alpha$ et $q = b + 2\beta$, fiet $a = 1$ et $b = 1$ ideoque $aa + 3bb = 4 = nn'$, unde patet etiam n' fore $= 2$, ita ut nulla ulterior diminutio locum habere possit. Quoties ergo hoc evenit, tum non ipse numerus N, sed eius duplum $2N$ erit numerus formae $pp + 3qq$.

COROLLARIUM 3

Hoc eo magis clarum reddetur, si perpendamus formulam $pp + 3qq$, quando ambo numeri p et q sunt impares, non solum esse parem, sed etiam per 4 divisibilem, neque adeo impariter parem umquam esse posse formam $pp + 3qq$. Quoties ergo, uti his casibus usu venit, numerus $2N$ in forma $pp + 3qq$ contineatur, tum N semper erit numerus par eiusque semissis $\frac{1}{2}N$ seu pars quarta ipsius $2N$ in hac forma $pp + 3qq$ continebitur. Quoties enim uterque numerus p et q est impar, tum etiam $\frac{pp+3qq}{4}$ semper est numerus eiusdem formae, idque adeo in integris, quod quidem non tam facile perspicitur. Posito enim $p = 2r + 1$ et $q = 2s + 1$ prodit forma

$$\frac{pp+3qq}{4} = 1 + r + rr + 3s + 3ss,$$

quam generatim neutiquam in integris ad quadratum cum triplo quadrato reducere licet. Sequenti autem modo haec resolutio in genere institui poterit. Observo enim omnia quadrata imparia in hac forma $(4m + 1)^2$ contineri, siquidem pro m etiam numeri negativi admittantur; namque si m sit positivum, quadrata numerorum 1, 5, 9, 13 etc., quorum forma est $4i + 1$, resultant;

1) Confer propositiones 5—7 Commentationis 272 nota p. 224 laudatae. F. R.

sin autem m sit numerus negativus, tum quadrata numerorum 3, 7, 11, 15 etc., quorum forma est $4i-1$, oriuntur. Iam ponamus

$$pp = (4r+1)^2 \text{ et } qq = (4s+1)^2$$

eritque

$$\frac{pp+3qq}{4} = 1 + 2r + 4rr + 6s + 12ss,$$

quae manifesto ad hanc formam redigitur

$$(1 + r + 3s)^2 + 3(r-s)^2.$$

SCHOLION

His theorematibus praemissis id, quod nobis maxime est propositum, aggrediamur demonstraturi, *quod summae quatuor quadratorum nullos alios divisores admittant, nisi qui ipsi quoque sint summae quatuor quadratorum.* Ad similitudinem autem praecedentium theorematum lemma quoque praemitti oportet.

LEMMA 4

9. *Productum ex duobus pluribusve numeris, qui singuli sunt summae quatuor quadratorum, semper quoque per summam quatuor quadratorum exprimi potest.*

Sit tale productum

$$(aa+bb+cc+dd)(\alpha\alpha+\beta\beta+\gamma\gamma+\delta\delta)$$

et capiatur

$$A = a\alpha + b\beta + c\gamma + d\delta,$$
$$B = a\beta - b\alpha - c\delta + d\gamma,$$
$$C = a\gamma + b\delta - c\alpha - d\beta,$$
$$D = a\delta - b\gamma + c\beta - d\alpha$$

horumque quadratorum summa erit

$$A^2 + B^2 + C^2 + D^2 = (a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2);$$

manifestum enim est singula producta ex binis partibus se mutuo destruere et singula quadrata litterarum latinarum in singula graecarum duci.[1])

1) Vide § 93 Commentationis 242 nota 2 p. 218 laudatae, imprimis notam ibi adiectam. F. R.

THEOREMA 4

Si N fuerit divisor cuiuspiam summae quatuor quadratorum seu formae $pp + qq + rr + ss$, quae quidem singula per N non sint divisibilia, tum N certe erit summa quatuor quadratorum.

DEMONSTRATIO

Non parum iuvabit hic quoque notasse quatuor illas radices p, q, r, s infra semissem numeri propositi N deprimi posse; demonstratio autem sequenti modo procedet.

I. Denotante n quotum ex illa divisione resultantem, ut sit

$$Nn = pp + qq + rr + ss,$$

ubi litterae p, q, r, s ita ad n referantur, ut sit

$$p = a + n\alpha, \quad q = b + n\beta, \quad r = c + n\gamma, \quad s = d + n\delta,$$

evidens omnino est litteras a, b, c, d ita sumi posse, ut $\frac{1}{2}n$ non superent, quandoquidem valores negativi hinc non excluduntur. Sicque formula $aa + bb + cc + dd$ certe minor erit quam nn.

II. His autem valoribus substitutis aequatio nostra erit

$$Nn = aa + bb + cc + dd + 2n(a\alpha + b\beta + c\gamma + d\delta) + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta),$$

quae ex lemmate praemisso, ubi posuimus

$$A = a\alpha + b\beta + c\gamma + d\delta,$$

ita contrahitur

$$Nn = aa + bb + cc + dd + 2nA + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

Quia ergo hic pars prima $aa + bb + cc + dd$ factorem habere debet n, statuatur

$$aa + bb + cc + dd = nn'$$

eritque omnino $n' < n$, uti modo ostendimus. Facta ergo divisione per n obtinebimus

$$N = n' + 2A + n(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

III. Multiplicemus nunc per n', et quia $nn' = aa + bb + cc + dd$, habebimus ex lemmate praemisso

$$nn'(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta) = A^2 + B^2 + C^2 + D^2,$$

qua forma introducta nostra aequatio erit

$$Nn' = n'n' + 2n'A + A^2 + B^2 + C^2 + D^2,$$

quae manifesto ad haec quatuor quadrata reducitur

$$Nn' = (n' + A)^2 + B^2 + C^2 + D^2.$$

IV. Quatenus igitur hic $n' < n$, eodem modo ad formas continuo minores Nn'', Nn''' etc. pertingere licebit, donec tandem ad formam $N \cdot 1$ perveniatur ideoque numerus propositus N quatuor quadratis aequetur.

COROLLARIUM 1

Hoc ratiocinium iterum levi exceptioni est obnoxium, quando scilicet fuerit $n = 2$ omnesque numeri p, q, r, s impares; tum enim fiet $a = 1$, $b = 1$, $c = 1$ et $d = 1$ hincque $nn' = 4$, ita ut quoque fiat $n' = 2$ sicque non minor quam n. Verum quum hinc numerus $2N$ aequetur summae quatuor quadratorum, aliunde perspicuum est etiam semissem N fore summam quatuor quadratorum, ita ut haec exceptio nihil plane turbare sit censenda.

COROLLARIUM 2

Quo hoc clarius perspiciatur, sint numeri p, q, r, s impares et n numerus par; tum, quia $Nn = pp + qq + rr + ss$, erit

$$\frac{1}{2}Nn = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 + \left(\frac{r+s}{2}\right)^2 + \left(\frac{r-s}{2}\right)^2,$$

quae quatuor quadrata itidem erunt integra; qua reductione uti licebit, quamdiu omnes radices quatuor quadratorum fuerint impares; tum autem exceptio ante memorata sponte concidit.

SCHOLION

Hac demonstratione potissimum theorema illud FERMATIANUM conficitur, quandoquidem altera pars, quae adhuc superest, quod scilicet proposito quo-

cumque numero primo semper summae quatuor quadratorum exhiberi queant per illum divisibiles, a me iam dudum[1]) satis clare est expedita atque adeo nuper a Celeb. LAGRANGE[2]) subtilissima demonstratione est firmata. Ut tamen hoc argumentum penitus conficiam, sequentem demonstrationem admodum facilem hic subiungam.

THEOREMA 5

10. *Proposito quocumque numero primo N non solum quaterna quadrata, verum adeo terna quadrata infinitis modis exhiberi possunt, quorum summa sit divisibilis per istum numerum N neque tamen singula per eum dividi queant.*

DEMONSTRATIO

Respectu numeri N omnes plane numeri in aliqua sequentium formarum continentur

$$\lambda N,\ \lambda N+1,\ \lambda N+2,\ \lambda N+3,\ \ldots\ \lambda N+N-1,$$

quarum numerus est N. Seposita autem prima forma, quae multipla ipsius N continet, circa reliquas, quarum numerus est $N-1$, notandum est quadrata primae formae $\lambda N+1$ et ultimae $\lambda N+N-1$ ad eandem formam $\lambda N+1$ redire, quadrata vero secundae formae $\lambda N+2$ et penultimae $\lambda N+N-2$ ad formam $\lambda N+4$, tertiae vero et antepenultimae ad $\lambda N+9$ redigi, et ita porro, ita ut hae tantum formae

$$\lambda N+1,\quad \lambda N+4,\quad \lambda N+9\quad \text{etc.},$$

quarum numerus est $\frac{1}{2}(N-1)$, quadrata in se complecti queant, quas formas primae classis appellemus et ita designemus

$$\lambda N+a,\quad \lambda N+b,\quad \lambda N+c,\quad \lambda N+d\quad \text{etc.},$$

ita ut litterae a, b, c, d etc. vel ipsa quadrata 1, 4, 9, 16 etc. denotent vel, si numerum N excedant, residua ex divisione restantia. Reliquae vero formae, quarum numerus itidem erit $\frac{1}{2}(N-1)$, hoc modo designentur

$$\lambda N+\alpha,\quad \lambda N+\beta,\quad \lambda N+\gamma,\quad \lambda N+\delta\quad \text{etc.},$$

1) Vide paragraphos 90 et 91 Commentationis 242 nota 2 p. 218 laudatae. F. R.

2) Vide notam 3 p. 218. F. R.

quas formas posterioris classis vocabimus. De his autem geminis classibus tres sequentes proprietates notentur, quas quidem facile demonstrare licet.[1])

I. Productum ex binis numeris primae classis itidem in prima classe continetur, scilicet forma $\lambda N + ab$ in prima classe reperietur; si enim ab maius fuerit quam N, eius loco residuum ex divisione per N facta relictum capi est intelligendum.

II. Numeri primae classis a, b, c, d etc. in quemcumque numerum posterioris classis α, β, γ, δ etc. ducti in classem posteriorem incident.

III. Denique producta ex binis numeris posterioris classis, veluti $\alpha\beta$, in classem primam transferuntur.

His praemissis demonstrabo: Si non darentur terna quadrata, quorum summa divisibilis esset per N, tum maximum absurdum inde esse secuturum. Ad hoc concedamus tantisper adversario nulla dari terna quadrata, quorum summa sit divisibilis per N; multo minus ergo duo talia quadrata dabuntur. Hinc statim sequitur formam $\lambda N - a$ sive, quod eodem redit, $\lambda N + (N - a)$ non in prima classe occurrere; si enim daretur quadratum formae $\lambda N - a$, hoc ad quadratum formae $\lambda N + a$ praeberet summam per N divisibilem, contra hypothesin. Forma igitur $\lambda N - a$ in posteriore classe contineatur necesse est sicque inter litteras α, β, γ, δ etc. reperientur numeri -1, -4, -9 etc. Sit f numerus quicumque primae classis, ita ut dentur quadrata formae $\lambda N + f$; ad quae si addantur quadrata formae $\lambda N + 1$, summa binorum habebit formam $\lambda N + f + 1$. Iam si daretur quadratum formae $\lambda N - f - 1$, haberetur summa trium quadratorum per N divisibilis; quod quum negetur, forma $\lambda N - f - 1$ non in prima classe ideoque in posteriori continebitur; in qua ergo quum reperiantur numeri -1 et $-f-1$, eorum productum $+f+1$ in priori classe occurrat necesse est. Simili modo ostendetur in prima classe quoque occurrere debere numeros

$$f + 2, \quad f + 3, \quad f + 4 \quad \text{etc.};$$

quare sumto $f = 1$ in prima classe occurrerent omnes plane formae

$$\lambda N + 1, \quad \lambda N + 2, \quad \lambda N + 3 \quad \text{etc.}$$

1) Demonstrationes inveniuntur in Commentatione 242 nota 2 p. 218 laudata. F. R.

nullaeque penitus pro classe posteriore relinquerentur. Interim tamen eodem ratiocinio vidimus in classe posteriore occurrere numeros

$$-1, \quad -f-1, \quad -f-2 \text{ etc.}$$

ideoque etiam omnes plane formas; quod quum sit maxime absurdum, sequitur falsum esse non dari terna quadrata, quorum summa sit divisibilis per numerum propositum N. Dantur ergo omnino terna multoque magis quaterna huiusmodi quadrata, quorum summa per N erit divisibilis.[1])

COROLLARIUM

Ex hoc theoremate cum praecedente coniuncto manifesto sequitur omnes plane numeros primos esse summas quatuor vel pauciorum quadratorum. Et quum producta ex binis pluribusve huiusmodi numeris eandem naturam sequantur, solidissime evictum est *omnes plane numeros esse summas quatuor quadratorum vel adeo pauciorum.*

SCHOLION

Loco huius propositionis Cel. LAGRANGE theorema multo latius patens in medium attulit et demonstratione munivit ingeniosissima quidem, sed tantopere abstrusa et intellectu difficili, ut nonnisi summa adhibita attentione percipi posset. Demonstravit scilicet proposito quocumque numero primo A semper bina quadrata pp et qq ad illum prima dari posse, ita ut formula $pp - Bqq - C$ per eum numerum primum A fiat divisibilis, quicumque numeri pro litteris B et C accipiantur, dummodo fuerint primi respectu ipsius A. Idem igitur theorema aliquanto latius extensum cum demonstratione longe faciliori et planiori hic subiungam.

THEOREMA 6

11. *Proposito quocumque numero primo N semper terna quadrata xx, yy et zz ad eum prima exhibere licet, ut formula*

$$\lambda xx + \mu yy + \nu zz$$

per numerum illum primum N fiat divisibilis, dummodo isti coefficientes λ, μ et ν ad ipsum N fuerint primi, hoc est, nullus eorum neque evanescat neque ipsi N neque eius multiplo cuipiam fuerit aequalis.

1) Confer § 90 Commentationis 242 nota 2 p. 218 laudatae. F. R.

DEMONSTRATIO

Denotent litterae

$$a,\ b,\ c,\ d \text{ etc.}$$

omnia residua, quae ex divisione quadratorum per numerum primum propositum N facta relinquuntur, quos numeros ante ad classem priorem rettulimus, quorum multitudo est $\frac{1}{2}(N-1)$; in iis scilicet omnes occurrunt numeri quadrati 1, 4, 9, 16 etc. minores quam N, maiorum autem residua illa ex divisione per N resultantia accedunt. Ad eandem vero classem etiam iidem numeri a, b, c, d etc. quovis multiplo numeri N aucti sunt referendi. Omnes autem reliqui numeri minores quam N, quorum numerus itidem est $\frac{1}{2}(N-1)$ quosque *non-residua*[1]) appellare licet, ad classem posteriorem sunt relati et litteris graecis

$$\alpha,\ \beta,\ \gamma,\ \delta \text{ etc.}$$

designentur. Circa hos numeros duplicis generis iam ante [§ 10] notavimus producta ex binis residuis seu classis prioris iterum in eandem classem cadere, veluti ab, ac, bc etc., quatenus scilicet per divisionem infra N deprimuntur, at productum ex residuo in non-residuum in classe posteriore non-residuorum reperiri ac denique producta ex binis non-residuis iterum fore residua. His notatis demonstrationem ita adornabimus, ut ostendamus ingens absurdum esse secuturum, si nulla daretur formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis. Demonstratio autem sequenti modo procedet.

I. Quum omnia quadrata aequentur cuipiam residuo a vel b vel c multiplo quodam numeri N aucto, si daretur talis formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis, ob $xx = \zeta N + a$, $yy = \eta N + b$ et $zz = \vartheta N + c$ foret utique formula $\lambda a + \mu b + \nu c$ per N divisibilis. Quare qui nostrum theorema negaverit, statuere debet nullam dari huiusmodi formulam $\lambda a + \mu b + \nu c$ per N divisibilem.

II. Quum igitur nulla detur huiusmodi formula per N divisibilis, multo minus fieri poterit $= 0$ ideoque ista aequatio $\lambda a = -\mu b - \nu c$ erit impossibilis pariter ac talis aequatio

$$\lambda a = (\zeta N - \mu)b + (\eta N - \nu)c.$$

1) Vide § 16 Commentationis 242 nota 2 p. 218 laudatae. F. R.

Verum quia λ, μ et ν sunt primi ad N, semper coefficientes ζ et η ita accipere licet, ut formulae $\zeta N - \mu$ et $\eta N - \nu$ fiant per λ divisibiles. Ponamus ergo

$$\zeta N - \mu = \lambda m \quad \text{et} \quad \eta N - \nu = \lambda n$$

atque impossibilis quoque erit ista aequatio

$$a = mb + nc.$$

III. Quum igitur ista formula $mb + nc$ non sit aequalis a ideoque in classe residuorum non reperiatur (secundum mentem scilicet adversarii, qui nostrum theorema negat), necessario in altera classe non-residuorum reperietur; ibidem ergo etiam (quia c unitatem denotare potest) occurret $mb + n$ hincque adeo omnes istae formulae

$$ma + n, \quad mb + n, \quad mc + n, \quad md + n \quad \text{etc.};$$

quae quum omnes a se invicem diversae et numero sint $\frac{1}{2}(N-1)$, his tota classis non-residuorum exhaurietur, quatenus scilicet divisae per N infra N deprimuntur.

IV. In eadem vero etiam classe occurrere debent omnia producta horum numerorum in quemlibet numerum primae classis, veluti d, ducta, quae ergo erunt

$$mad + nd, \quad mbd + nd, \quad mcd + nd \quad \text{etc.}$$

Verum producta ad, bd, cd etc. in priorem classem cadunt ac reperientur inter ipsos numeros a, b, c, d etc.; sicque in altera classe inter non-residua occurrent quoque omnes hae formulae

$$ma + nd, \quad mb + nd, \quad mc + nd \quad \text{etc.},$$

quae praecedentes singulas superant quantitate $n(d-1)$. Hoc discrimen ponatur brevitatis gratia $= \omega$, quod utique ad ipsum divisorem N erit primum, si modo pro d non assumatur unitas, quia $d - 1$ est $< N$ atque etiam numerus n primus ad N.

V. Quodsi igitur in classe non-residuorum contineatur numerus α, ibidem quoque occurret $\alpha + \omega$ atque ob eandem rationem hic numerus iterum incrementum ω accipiens, scilicet $\alpha + 2\omega$, ibi reperiatur necesse est atque ob

eandem rationem etiam numeri $\alpha + 3\omega$, $\alpha + 4\omega$ etc. Omnes igitur termini huius progressionis arithmeticae

$$\alpha, \quad \alpha + \omega, \quad \alpha + 2\omega, \quad \alpha + 3\omega \quad \text{etc.},$$

quatenus scilicet per N divisae infra N deprimuntur, inter non-residua occurrere debebunt.

VI. Quia differentia huius progressionis est ω, numerus scilicet ad N primus, in hac progressione occurrunt termini non solum per N divisibiles, sed etiam insuper omnes, qui per N divisi pro residuis praebent omnes plane numeros 1, 2, 3, 4 etc. nullo excluso.[1]) Quocirca secundum mentem adversarii in classe non-residuorum omnes plane occurrerent numeri 1, 2, 3, 4 etc.; quod quum sit absurdum, opinio adversarii certe est falsa. Scilicet falsum est nullos dari numeros formae

$$\lambda xx + \mu yy + \nu zz,$$

qui sint per N divisibiles. Utique igitur tales numeri dabuntur; atque hoc ipsum est, quod praestare suscepimus.

COROLLARIUM 1

Non solum autem semper tria huiusmodi quadrata xx, yy et zz reperire licet, sed etiam unum eorum, veluti zz, pro lubitu assumere licet, dumne sit per N divisibile. Ita si f denotet numerum pro lubitu datum non divisibilem per N, semper assignare licebit bina quadrata xx et yy, ut formula

$$\lambda xx + \mu yy + \nu ff$$

fiat per N divisibilis. Ad hoc demonstrandum, quicumque fuerit numerus z, semper dabitur eiusmodi numerus v, ut productum vz per N divisum relinquat datum residuum f. Sit enim $vz = \vartheta N + f$ et formula nostra per vv multiplicata, quae utique adhuc divisibilis erit per N, fiet

$$\lambda vvxx + \mu vvyy + \nu(\vartheta\vartheta NN + 2\vartheta Nf + ff),$$

---

1) Vide theorema 1 Commentationis 271 (indicis Enestroemiani): *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 531. F. R.